

# Ook deugdelijke stemmachines deugen niet

Paul Huygen

9 november 2006

## Samenvatting

Inmiddels heeft de stemcomputer bijna overal de stembiljetten vervangen. Daardoor zijn de verkiezingen niet meer door de burgers te controleren. Achteraf is er geen mogelijkheid om de juistheid van de verkiezingsuitslag aan te tonen.

## 1 Verkiezingen 2014

Het is 2014. Een krantenbericht meldt: “De rellen in Rotterdam over de verkiezingsuitslag hebben een grote ravage aangericht. Het gemeentebestuur probeert aan te tonen dat de stemmachines de uitslag goed hebben weergegeven. Maar een onafhankelijk onderzoek van twee hoogleraren van de prestigieuze Amerikaanse Princeton University wijst uit dat de uitslag niet geverifieerd kan worden.

De pas opgekomen partij “Lijst Piet Pauwels” wilde grootscheepse hervormingen. De partij had een hele grote aanhang, en zou volgens peilingen zeker 35% van de stemmen krijgen. Toen de partij slechts 20% van de stemmen kreeg ging het gerucht dat gemeenteambtenaren onder druk van derden met de stemmachines hadden geknoeid”.

## 2 Controleerbaarheid van verkiezingen

Vrije verkiezingen zijn een belangrijk kenmerk van een democratie. Het is essentieel dat de bevolking de verkiezingsuitslag kan vertrouwen en dus ook controleren. De procedure van de verkiezingen was in het verleden dan ook volledig transparant. Artikel J35 van de kieswet geeft iedere stemgerechtigde het recht om de zitting van een stembureau bij te wonen. Deze kan dan met eigen ogen zien dat de stembus eerst leeg verzegeld wordt, wie er iets in de stembus stopt en hoe er achteraf geteld wordt. Er is een bekende hoeveelheid stembiljetten in gebruik en achteraf kan vastgesteld worden dat het aantal daadwerkelijk gebruikte stembiljetten daarmee in overeenstemming is. De stembiljetten blijven bewaard en kunnen achteraf opnieuw geteld worden als er problemen zijn. Iedere burger kan dus de volgende drie kernonderdelen van de procedure met eigen ogen controleren: 1) wordt iedere stem juist geregistreerd?; 2) worden er geen “spookstemmen” gegenereerd? en 3) worden de uitgebrachte stemmen correct bij elkaar opgeteld?

Deze openheid behoort bij de internationale statuur van Nederland. Nederlanders maken vaak deel uit van internationale commissies die de legaliteit van verkiezingen in het buitenland controleren. Het zou dan vreemd zijn als de Nederlandse verkiezingen zelf niet controleerbaar zijn.

In 1989 zijn de artikelen J32 t/m J34 aan de de Kieswet toegevoegd. Deze doen de oorspronkelijk beoogde transparantie feitelijk teniet door de introductie van stemmachines. Nu kan niemand meer controleren of iedere stem juist wordt geregistreerd en of de stemmen juist worden opgeteld.

Op dit moment vertrouwt het overgrote deel van de Nederlandse kiezers (gelukkig) erop dat de overheid de verkiezingen zorgvuldig organiseert. Ze volgen de verkiezingen liever thuis achter de TV dan dat ze in het stemlokaal kijken of het tellen wel netjes verloopt. Maar kan de overheid demonstreren dat de verkiezingen betrouwbaar zijn als een aantal kiezers dat — in slechtere tijden — zou wensen?

De laatste weken is er veel onrust, omdat de stichting “Wij vertrouwen stemcomputers niet” in Nederland veelgebruikte stemmachines heeft onderzocht en allerlei veiligheidsrisico’s heeft aangetoond. Zo blijkt het voor buitenstaanders niet onmogelijk te zijn om de software in de machines (feitelijk computers) zodanig te veranderen dat de verkiezingsresultaten ongemerkt vervalst worden, en blijkt het mogelijk om straling uit de stemmachine op te vangen en daarmee te bepalen op wie een kiezer heeft gestemd<sup>1</sup>. Uit de reactie van de verantwoordelijke minister blijkt dat de overheid dit als een technisch probleem ziet, dat opgelost moet worden door extra controles, verzegeling van de stemmachines en veiliger opslag. Maar ook met de beste technische oplossingen blijven stemmachines “black boxes”, waarvan maar een klein groepje ingewijden het inzicht heeft om te kunnen beoordelen of ze doen wat ze moeten doen. De kiezers kunnen het niet meer zelf controleren. Achteraf kan niemand aantonen dat de uitslag van de stemmachines correct was.

### 3 Gebruik van stemmachines

In Nederland kopen of huren overheden stemmachines van particuliere bedrijven. Negentig procent van de Nederlandse gemeentes gebruikt stemmachines van één fabrikant, Nedap-Groenendaal te Groenlo<sup>2</sup>. Voordat een stemmachine gebruikt mag worden moet het type eerst goedgekeurd worden door een door de Minister van Binnenlandse Zaken aangewezen keuringsinstelling<sup>3</sup>. Momenteel is er één aangewezen keuringsinstelling, Brightsight. De fabrikant laat eerst een prototype van een nieuw type stemmachine keuren. Na goedkeuring daarvan stelt de fabrikant tien machines ter beschikking, waarvan de keuringsinstelling één willekeurig geselecteerd exemplaar onderzoekt. De laatste keuringsprocedure moet iedere vier jaar herhaald worden. De keuringsinstelling krijgt de beschikking over de volledige technische documentatie en de broncode van de software<sup>4</sup>.

Gemeentes kunnen goedgekeurde stemmachines inzetten bij verkiezingen. De rest van de tijd worden de machines opgeslagen. Aan deze opslag werden tot nu toe alleen technische eisen gesteld, zoals temperatuur en vochtigheid.

De Nedap stemmachines zijn feitelijk gespecialiseerde computers<sup>5</sup> In de stemmachine wordt voor de verkiezingen een elektronisch onderdeel, de stemurn, geschoven.

---

1. Computerbeveiligingsdeskundige Bart Jacobs schreef [5] over deze potentiële inbreuk op het stemgeheim “Dit is een principieel punt: je zou stemcomputers ook onder Saddam Hoessein moeten durven gebruiken”

2. Volgens de website van Nedap-Groenendaal

3. Regeling voorwaarden en goedkeuring stemmachines 1997

4. Overigens is deze documentatie en de broncode van de software bedrijfsgeheim, niet toegankelijk voor derden

5. de stichting “Wij vertrouwen stemcomputers niet” heeft twee stemmachines van een gemeente gekocht en onderzocht. Een gedetailleerde beschrijving ervan staat in <http://www.wijvertrouwenstemcomputersniet.nl/Nedap>.

Deze stemurn is een los geheugen. Vóór de verkiezing wordt hij op een aparte computer in een centraal stembureau gevuld met informatie over de verkiezingen (welke partijen zijn er, en welke kandidaat zit onder welke knop). Tijdens de verkiezing verzamelt de stemurn de stemtotalen, die achteraf in de computer van het centrale stembureau kunnen worden uitgelezen.

Bij het stemmen drukt de kiezer op de knop van de gekozen kandidaat. De naam en de partij van de kandidaat verschijnen in het uitleesvenster. De kiezer kan dat controleren en vervolgens stemmen door op een “akkoord” knop te drukken. Met een los bedieningskastje geeft een medewerker van het stembureau telkens de stemmachine vrij zodat een kiezer één stem kan uitbrengen.

Aan het einde van de stemming drukt een in de stemmachine ingebouwde printer een lijst af van de aantallen stemmen per kandidaat. Vervolgens wordt de stemurn in een envelop gestoken en naar het centrale stembureau van het stembedistrict gebracht.

## 4 Oncontroleerbaarheid van stemmachines

De controle mogelijkheden van de stemgerechtigde burger zijn bij stemmachines behoorlijk ingeperkt. Op het stembureau is het enige dat hij nog kan controleren, of het aantal door de stemmachine geregistreerde stemmen gelijk is aan het aantal uitgebrachte stemmen. Maar hij kan niet controleren of de stemmen juist geregistreerd zijn.

De volgende zaken die kunnen veroorzaken dat de stemuitslag van een stemmachine onjuist is, vallen buiten het zicht van stemgerechtigde burgers:

### 4.1 Is de machine juist geconstrueerd?

De constructie van de stemmachine is normaal gesproken ontoegankelijk voor buitenstaanders<sup>6</sup>. Daardoor kan de kiezer niet met eigen ogen zien hoe betrouwbaar de constructie van de machine is, maar moet hij afgaan op de deskundigheid en de integriteit van de fabrikant en de medewerkers van de keuringsinstelling<sup>7</sup>. Op dit moment is de betrouwbaarheid van de constructie van de Nedap stemmachines wel bekend door het onderzoek van stichting “Wij vertrouwen stemcomputers niet” [3]. De Stichting heeft een officieel verzoek ingediend bij de burgemeester van Amsterdam om een van de in deze stad gebruikte machines<sup>8</sup> te onderzoeken, maar de burgemeester heeft dat verzoek afgewezen omdat de fabrikant dat niet toestaat.

### 4.2 Software

Een stemmachine is feitelijk een gespecialiseerde computer, waarin software bepaalt wat de machine precies doet. De broncode van de software in de Nedap stemmachine beslaat ongeveer 20000 regels<sup>9</sup>. Veel experts schatten, dat ook uitgebreid geteste software, die door deskundige programmeurs is geschreven al snel ongeveer 10 fouten per duizend regels code bevat<sup>10</sup>. Het zou dus niet vreemd zijn als de software

---

6. Stichting “Wij vertrouwen stemcomputers niet” heeft zichzelf wel toegang verschaft door twee stemmachines van een gemeente te kopen, zogenaamd om er ondernemingsraadverkiezingen mee te gaan houden.

7. Ook de overheid zelf heeft geen inzicht meer in de betrouwbaarheid van de stemmachines. Zij heeft de verantwoordelijkheid hiervoor helemaal aan de fabrikant en het keuringsbedrijf overgedragen.

8. Amsterdam gebruikt SDU stemmachines

9. verklaring van de voor de verkiezingssystemen verantwoordelijke persoon bij Nedap in [9]

10. Schattingen over het aantal te verwachten fouten lopen nogal uiteen. De genoemde schatting is afkomstig van [4]. Het zijn altijd ondergrenzen, gebaseerd op nauwkeurige analyse van representatieve steekproeven uit gebruiksklare software

in Nedap stemmachines ongeveer tweehonderd fouten bevat. Alleen door grondig testen kan vertrouwen verkregen worden dat deze fouten in de meest-voorkomende situaties geen invloed hebben op de werking van het apparaat<sup>11</sup>. Volledige zekerheid dat er nooit fouten zullen optreden is niet te geven. De kiezer moet er dus op vertrouwen dat de stemmachine zo grondig getest is dat de kans op het optreden van fouten verwaarloosbaar is.

Verder zou er gebruik gemaakt kunnen zijn van zogenaamde “achterdeurtjes”. Programmeurs brengen deze achterdeurtjes vaak aan in software voor apparaten als stemmachines. Deze maken het voor technici mogelijk om bijzondere dingen te doen. Een achterdeurtje kan er bijvoorbeeld voor zorgen dat als iemand tegelijkertijd bepaalde knoppen indrukt de machine in een speciale modus springt. Een achterdeurtje kan natuurlijk ook met kwade bedoelingen zijn aangebracht. De kiezer moet er op vertrouwen dat er geen achterdeurtjes in de software zitten en, als die er toch in zitten, niemand er misbruik van heeft gemaakt.

### 4.3 Zit de stemmachine in elkaar zoals hij in elkaar hoort te zitten?

De keuringsinstelling keurt niet iedere stemmachine, maar alleen een paar door de fabrikant ter beschikking gestelde exemplaren. Dat betekent dat de kiezer er op moet vertrouwen dat de fabrikant de stemmachine goed in elkaar gezet heeft, en dat naderhand niemand met de stemmachine geknoeid heeft. Dat laatste nu is lastig.

Achteraf is het vaak niet mogelijk om te controleren of er niet met de stemmachine geknoeid is. Uit het onderzoek van stichting “Wij vertrouwen stemcomputers niet” blijkt dat de software in de Nedap computers op losse, verwisselbare chips (e-proms) zit, die bij de verkiezingen door kwaadwillenden tijdelijk door andere chips, met software die de verkiezingen vervalst, vervangen zouden kunnen worden. Onderzoekers van Princeton University [2] hebben aangetoond dat bij in Amerika veelgebruikte stemmachines<sup>12</sup> software ingevoerd kan worden die de verkiezingsuitslag kan vervalsen om daarna, zonder sporen achter te laten, zichzelf uit het geheugen te wissen. Uit een TV-reportage<sup>13</sup> blijkt bovendien, dat de stemmachines van de gemeente Rotterdam tussen de verkiezingen door onbeveiligd zijn opgeslagen, zodat gemotiveerde buitenstaanders de gelegenheid hebben om de software in de stemmachines te veranderen.

Zelfs als de software in de stemmachine blijvend veranderd is, kan dit moeilijk tot onmogelijk op te sporen zijn. De veranderingen kunnen zodanig zijn, dat de machine zich alleen in bijzondere situaties anders gaat gedragen (bijvoorbeeld na activering van een achterdeurtje door een medeplichtige stemmer), en dat computerprogramma's die de software moeten controleren voor de gek gehouden worden<sup>14</sup>.

De onthullingen van Stichting “Wij vertrouwen stemcomputers niet” en van het televisieprogramma “één vandaag” laten zien, dat op dit moment de Nederlandse stemmachines zo slecht beveiligd zijn, dat kwaadwillende buitenstaanders zeer goed in staat moeten worden geacht om verkiezingen te vervalsen. Maar ook als de stemcomputers volgens de huidige maatstaven technisch optimaal in elkaar zouden zitten, is de betrouwbaarheid van de stemmachines afhankelijk van slechts een klein groepje ingewijden dat de stemmachines maakt, keurt en beheert. Niet alleen de goede trouw van deze personen is van belang, maar ook hun alertheid om te

---

11. Een Ierse onderzoekscommissie vond in 2004 nog een softwarefout in Nedap stemmachines [6] die tot telfouten zou kunnen leiden. Dat was een van redenen voor een advies om deze stemmachine niet te gebruiken bij de volgende verkiezingen

12. Diebold AccuVote

13. Televisieprogramma “één vandaag” van 4 oktober 2006

14. Hackers veranderen zo veel computers die aan Internet verbonden zijn met “root kits”

voorkomen dat onbevoegden de apparaten kunnen veranderen. Als een deel van de kiezers deze personen niet meer vertrouwt, kan niemand hen aantonen dat de verkiezingen toch eerlijk verlopen zijn.

#### 4.4 Audit van kritische IT systemen

Deskundigen op het gebied van automatisering wijzen bepaalde IT-toepassingen aan als kritisch. Deze systemen hebben een grote invloed op belangrijke, kostbare, processen. Een eis die gesteld wordt aan kritische systemen is, dat achteraf altijd gecontroleerd kan worden of het systeem wel goed gewerkt heeft. Een systeem dat bijvoorbeeld automatisch beslissingen over uitkeringen neemt, moet de beslissingen kunnen uitleggen. Bij fouten kunnen rechters dan de beslissingen ongedaan maken. Een gelduitgifteautomaat biedt ook mogelijkheden voor controle achteraf. In het automaat zit een getelde hoeveelheid geld, alle transacties worden geregistreerd en achteraf kan gecontroleerd worden of de som van de uitgegeven hoeveelheid geld overeenkomt met de hoeveelheid geld die verdwenen is.

Als belangrijke schakel in de procedure om de regering van het land te constitueren zou de stemmachine als kritisch IT-systeem gekwalificeerd moeten worden. Maar in tegenstelling tot andere kritische informatiesystemen zijn er bij stemmachines achteraf geen controlemogelijkheden buitenom het IT-systeem zelf [8].

De Internationale instelling die waarnemers uitzendt om de eerlijkheid van verkiezingen te controleren, de “Office for Democratic Institutions and Human Rights” van de OSCE, keurt vanwege het gebrek aan controlemogelijkheden stemmachines zonder “paper trail” af<sup>15</sup>. Wat moet een Nederlandse OSCE waarnemer zeggen als zijn bezwaar verworpen wordt omdat hij immers in zijn eigen land ook op deze manier stemt?

## 5 Alternatieven

Op dit moment hebben stemmachines niet de transparantie van de ouderwetse stembiljetten. Als wij met de huidige stand van de techniek willen bereiken dat burgers de verkiezingen kunnen controleren, dan lijkt de enige weg te zijn, er voor te zorgen dat iedere stem een telbaar stembiljet achterlaat. De voor de hand liggende oplossing is dus, om weer terug te gaan naar stembiljetten. Het grootste nadeel daarvan is, dat het veel meer tijd kost tot de uitslag bekend is. Maar er is een alternatief. Het is mogelijk om stemmachines te gebruiken die in staat zijn om een stembiljet te drukken. De kiezer controleert het stembiljet en stopt het in een stembus. Steekproefsgewijs kunnen dan de papieren biljetten geteld worden en de uitslag vergeleken met die van de machine. Het voordeel dat de verkiezingsuitslag vanwege de stemcomputer snel bekend is, blijft dan behouden<sup>16</sup>. Wellicht dat later alternatieve methoden voor elektronisch stemmen [1], gebaseerd op encryptiemethoden, ontwikkeld kunnen worden die zo transparant zijn dat burgers ze kunnen controleren.

## 6 Conclusie

De kieswet regelde vóór 1989 de verkiezingen zodanig dat kiesgerechtigden deze konden controleren. Door de introductie van de stemmachine is deze transparantie

---

15. het handboek [7], bladzijde 43, noemt zulke stemmachines een risicofactor

16. Dit wordt ook bepleit door stichting “Wij Vertrouwen Stemcomputers Niet”

voor een groot deel ongedaan gemaakt. Burgers moeten nu vertrouwen op de deskundigheid en integriteit van een klein groepje betrokkenen. Achteraf is het zelfs voor auditspecialisten onmogelijk om vast te stellen of de verkiezingsuitslag juist is.

Was de wetgever vóór 1989 onnodig paranoïde, of stelt hij nu te veel vertrouwen in een klein groepje deskundigen en ambtenaren? De in Nederland gebruikte stemmachines zouden eigenlijk pas ingevoerd mogen worden na een fundamentele discussie over dit punt en een uitspraak waarom de transparantie die tot dusver werd nagestreefd nu niet meer nodig is. Het fictieve voorbeeld aan het begin van dit artikel geeft een voorbeeld van omstandigheden waaronder verkiezingen geverifieerd zouden moeten worden. Daarvoor is het nodig dat iedere stem een controleerbaar artefact, zoals een stembiljet, achterlaat.

## Referenties

- [1] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, pages 38–47, januari/februari 2004.
- [2] A.J. Feldman, J.A. Halderman, and E.W. Felten. Security analysis of the diebold accuvote-ts voting machine. In press. <http://itpolicy.princeton.edu/voting/ts-paper.pdf>, september 2006.
- [3] R. Gonggrijp, W.-J. Hengeveld, A. Bogk, D. Engling, H. Mehnert, F. Rieger, P. Scheffers, and B. Wels. Nedap/groenendaal es3b voting computer: a security analysis. Technical report, Stichting “Wij vertrouwen stemcomputers niet”, 2006. <http://www.wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf>.
- [4] W.S. Humphrey. The software quality profile. Technical report, Carnegie Mellon University, 2004. <http://www.sei.cmu.edu/publications/articles/quality-profile/index.html>.
- [5] Bart Jacobs. Stemcomputer vraagt om fraude. *NRC-Handelsblad*, (11-10-2006), 2006.
- [6] Commission on Electronic Voting. First report on the secrecy, accuracy and testing of the chosen electronic voting system. Technical report, Government of Ireland, 2004. [http://www.cev.ie/htm/report/download\\_first.htm](http://www.cev.ie/htm/report/download_first.htm).
- [7] OSCE. *Election Observation Handbook*, fifth edition, 2005. [http://www.osce.org/odihr-elections/item\\_11\\_14004.html](http://www.osce.org/odihr-elections/item_11_14004.html).
- [8] E.J.M. Ridderbeekx. Elektronisch stemmen: een auditperspectief. *de EDP-Auditor*, (2):20–32, 2006.
- [9] A. Zebregs. Tweegesprek op toernooiveld in nijmegen (deel 2). *Burgerzaken en Recht*, (10):366–367, oktober 2004.